BIG BROTHER ON DUTY: HUMAN RIGHTS CONCERNS ON BIOMETRIC FACIAL RECOGNITION FOR CRIME PREVENTION*

Büyük Birader İş Başında:
Suç Önleme Amaçlı Biyometrik Yüz Tanımaya İlişkin İnsan Hakları Sorunları

Neslihan CAN YAVUZ**

L&IR
Year: 17, Issue: 31
January 2026
pp.27-46

Article Information

Submitted	*: 1.7.2025*
Revision Requested	*:13.10.2025*
Last Version Received	*: 18.10.2025*
Accepted	*: 30.10.2025*

Article Type

Research Article

Abstract

Smart technologies, which permeate every aspect of our daily lives today, not only detect criminals but also prevent them. Since the innovation of artificial intelligence (AI) and biometric technologies, there has been a significant increase in the recording and storage of personal data, particularly in terms of data protection. The use of the aforementioned technologies by law enforcement and other judicial authorities raises issues of interference with individuals' right to respect for private life under the European Convention on Human Rights. In the literature, this use has been studied in relation to the right to respect for private life, the right to the protection of personal data, the regime of interference, the criminal consequences of unlawful use, and the issue of compensation for the violation. However, the effects of the use of biometric-based facial recognition systems for the purpose of crime prevention on human rights have not been subject to theoretical and critical evaluation. This study raises a critical question as to whether these systems will lead to a future like the dystopia described in Orwell's 1984, and aims to examine if the states' processing of biometric data, primarily through facial recognition technologies (FRTs), is leading us towards a dystopia or a utopia where crimes are minimized. The study delves into both the shortcomings and efficiency of facial recognition systems by pointing out the related case law of the European Court of Human Rights (ECtHR).

Keywords: Facial recognition technology, biometric data, crime prevention, right to privacy, European Court of Human Rights

---

* There is no requirement of Ethics Committee Approval for this study.
This study is an expanded and revised version of the paper presented at the 3rd Information Technology Law Symposium on "Artificial Intelligence and Law," organized by the Faculty of Law of Ankara Social Sciences University on May 29, 2024.

** Asst. Prof., Recep Tayyip Erdoğan University Faculty of Law, Department of Criminal and Criminal Procedure Law, E-Mail: neslihan.can@erdogan.edu.tr, ORCID: 0000-0002-6990-8274.

Özet

Günlük hayatın her alanına nüfuz eden akıllı teknolojiler, günümüzde yalnızca suçluları tespit etmekle kalmayıp aynı zamanda önlemeye matuf olarak kullanılmaktadır. Yapay zekâ ve biyometrik teknolojilerin gelişmesiyle de özellikle veri koruma alanında kişisel verilerin kaydedilmesi ve saklanmasında önemli bir artış olmuştur. Mezkûr teknolojilerin kolluk ve diğer adli makamlar tarafından kullanımı, bireylerin Avrupa İnsan Hakları Sözleşmesi'nin özel hayata saygı hakkı kapsamında müdahaleleri gündeme getirmektedir. Nitekim literatürde bu kullanım özel hayata saygı hakkı ve daha özelde kişisel verilerin korunması hakkı bağlamında müdahale rejimi itibarıyla incelendiği gibi hukuka aykırı kullanımların suç tipi olarak karşılıkları veya ihlalin giderimine ilişkin tazminat meselesi ele alınmıştır. Fakat özellikle biyometrik tabanlı yüz tanıma sistemlerinin suçların önlemesi amaçlı olarak kullanımının insan hakları üzerindeki etkileri kuramsal ve kritik bir değerlendirmeye tabi tutulmuş değildir. Bu çalışma ise bu sistemlerin Orwell'ın 1984 distopyasındaki gibi bir geleceğe yol açıp açmadığına dair kritik bir soruyu gündeme getirmekte ve devletlerin başta yüz tanıma teknolojileri olmak üzere biyometrik verileri işlemesinin toplumu bir distopyaya mı yoksa suçların en aza indirildiği bir ütopyaya mı götürdüğünü incelemeyi amaçlamaktadır. Çalışma, Avrupa İnsan Hakları Mahkemesi'nin ilgili içtihadına işaret ederek yüz tanıma sistemlerinin hem eksikliklerini hem de etkililiğini ele almaktadır.

Anahtar Kelimeler: Yüz tanıma teknolojisi, biyometrik veri, suç önleme, özel hayat hakkı, Avrupa İnsan Hakları Mahkemesi

INTRODUCTION

"*The poster with the enormous face gazed from the wall. It was one of those pictures which are so contrived that the eyes follow you about when you move. BIG BROTHER IS WATCHING YOU*"[1]

Being vastly applicable in computer network login to e-commerce, driving licence to social security, border checkpoints, without any doubt the use of biometrics is a part of ordinary life. Yet, the tight connection between biometrics and commercial sphere and governmental sphere did not remain far away from law enforcement purposes to be utilized[2]. Imagine that you are going to work on

1 George Orwell, *1984* (Arcturus Publishing, 2013) 9.

2 *Jain et al* divided the applications of biometrics into three categories: commercial applications, including internet access, medical records management, and distance learning; governmental applications, including passport controls and ID cards; and lastly, forensic applications, including law enforcement purposes, such as terrorist identification, criminal investigation, and other purposes related to missing children and parenthood determination. See Anil K. Jain, Arun Ross, and Salil Prabhakar, 'An Introduction to Biometric Recognition' (2004) 14 (1) IEEE Transactions on Circuits and Systems for Video Technology 11; Another classification

an ordinary day. At the moment you walk down the street, the surveillance camera starts to watch and record you. Only the surveillance camera? The police officers wearing smart glasses quickly scan you and the hundreds of people waiting for the subway at the station. The glasses then send the captured images of these people to a facial recognition database, which then compares these images with those for whom an arrest warrant has been issued. Two police officers wearing smart glasses come near you and arrest not you but a couple of persons at the station. Interestingly, all of this occurred in just a few seconds.

Now turning back to the reality, 33 suspects have been detained in Zhengzhou, China, exactly the same way[3]. In China, public surveillance is everywhere, from banks to airports. By the end of 2018, there were 200 million surveillance monitors in China, and this number is expected to increase to approximately 626 million by 2020. The widespread application of FRT for the sake of public safety, prevention of crime or solving crime is not peculiar to China, considering emergence of FRT's use corresponded right after the 9/11 attacks in the USA with SmartGate technology[4]. Thus, *Feldstein*'s study, which collected data and findings from 176 countries, confirms that at least 75 of the sample countries actively apply AI technologies for the following purposes: 56 for smart/safe cities, 64 for facial recognition systems, and 52 for smart policing[5].

Until now, the legal academia's perspective on the processing of personal data has been diverse, ranging from advocating for a dystopian future with privacy concerns, to legal scholars who have shifted their focus to biometric or genetic data. These scholars appear to be satisfied with the use of DNA samples and the processing of personal data to solve serious crimes, as well as less serious ones such as theft or property damage. However, domestic authorities often

---

as *Marciano* splendidly charted a surveillance network with the elements that are divided into five levels, respectively: (1) states over both citizens or non-citizens in the context of national security, public services, and welfare; (2) institutions over wards in the context of prisons, schools, and hospitals; (3) employers over employees in the context of the workplace; (4) corporations over consumers in the context of markets; (5) individuals over sub-individuals in the context of their homes. See Avi Marciano, 'Reframing biometric surveillance: from a means of inspection to a form of control' (2019) (21) Ethics and Information Technology 128.

3 Springwise, 'Chinese Police Adopt Smart Glass Technology' (2018) <https://www.springwise.com/chinese-police-adopt-smart-glass-technology/#:~:text=Using%20facial%20recognition%20technology%2C%20these,technology%20to%20assist%20police%20work> accessed 15 December 2024.

4 Marcus Smith and Monique Mann, 'Facial Recognition Technology and Potential for Bias and Discrimination' in Rita Matulionyte and Monika Zalnieriute (eds) *The Cambridge Handbook of Facial Recognition In The Modern State*, (Cambridge University Press, 2024) 88.

5 Steven Feldstein, 'The Global Expansion of AI Surveillance' (2019) Carnegie Endowment For International Peace <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en> accessed 21 December 2024 7.

maintain the belief that the use of biometric technologies serves public safety and has no connection to privacy issues[6]. Police officers in Beijing's outskirts use smart glasses created by LLVision, which scan the faces of vehicles and car plates before sending the data to the central system. When a face matches the blacklist, it triggers a warning signal. Wu Fei, the chief executive of LLVisions asserts that China employs this technology for noble objectives. According to Wu Fei, this system ensures people's privacy is not a concern[7].

Contrary to governments' purposes of the use of FRT for law enforcement, the discussions and concerns surrounding FRT span a wide range, including privacy and data protection, discrimination, the lack of transparency regarding the purposes of processed data, and the potential chilling effect on freedom of expression, peaceful marches, and assembly[8]. For instance, one of the concerns pertains to a predictive crime forecasting algorithm known as PredPol. This algorithm gathers historical criminal events from departments into datasets, directing police attention towards high-risk areas. However, it also labels certain minority neighbourhoods, potentially leading to structurally biased policing in these areas[9]. Not only did the newly developed FRT tool raise concerns, but the European Court of Human Rights (ECtHR) also began considering FRTs due to similar concerns. This was evident in the case of *Glukhin v. Russia*, where facial recognition cameras detected the applicant, a peaceful solo demonstrator in the Moscow subway, and found him guilty of a minor offence for not informing public authorities about his demonstration. The ECtHR pursued its case law on peaceful demonstrations, concluding that there was no danger or major disruption of daily life, despite the absence of prior notification to public authorities[10]. Besides, the Court correlated the issue with FRTs and stated that intrusive use of FRT leads to a chilling effect on peaceful protests[11].

The ECtHR's jurisprudence traces these concerns to the use of biometric techniques. Since the landmark case of *S. and Marper v. the United Kingdom*,

---

6 Rahime Erbas, 'DNA Databases For Criminal Justice System: A Pathway Towards Utopian or Dystopian Future?' (2022) (18) The Age of Human Rights Journal 331-332.

7 Pie Li and Cate Cadell, 'China Eyes 'Black Tech' To Boost Security As Parliament Meets' (Reuters, 2018) <https://www.reuters.com/article/technology/china-eyes-black-tech-to-boost-security-as-parliament-meets-idUSKBN1GM06M/> accessed 15 December 2024.

8 Rita Matulionyte and Monika Zalnieriute, *The Cambridge Handbook of Facial Recognition In The Modern State*, (eds) Rita Matulionyte and Monika Zalnieriute (Cambridge University Press, 2024) 1-2; Neil Shah, Nandish Bhagat and Manan Shah, 'Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention' (2021) 4 (9) Visual Computing for Industry, Biomedicine, and Art 3.

9 Feldstein (n 4) 20.

10 *Glukhin v. Russia*, Application no. 11519/20, 4 July 2023, paras. 56-57.

11 *Glukhin v. Russia*, para. 88.

where the Strasbourg Court found a violation of art. 8 in terms of the proportionality requirement by emphasising that the applicants were not convicted of the accused offences and the risks of misuse or abuse of retained data without any time limits[12] both legal scholars have discussed the relationship between biometric data processing and human rights violations.

This study aims to highlight the concerns surrounding the use of FRTs in a concise manner, adopting a sceptical and Orwellian stance towards the use of biometric technologies. Rather than adopting a jurisdictional approach, I prefer to focus on the concerns that the ECtHR briefly outlines. This is because citizens from all over the world living in states that apply FRTs face the risk of becoming trapped in totalitarian superstates like Oceania in 1984. Since the study focuses on human rights violations, the ECtHR's interference analysis method serves as the most effective method. This can demonstrate that the second step of the method legitimately aims to prevent crimes and capture criminals, while the third step, known as proportionality, also recognises privacy, discrimination, and incorrect matches on biometric technologies as legitimate goals. Excluding a domestic-jurisdictional approach may lead to a strict reliance on domestic law for the definition of legality, thereby taking the legality of interference, the first step in the ECtHR's methodology, for granted. Furthermore, the study limits itself to considering only the biometric data processed with the aim of crime prevention, as the current trends in criminal justice and the use of biometric technologies tend to favor ex-ante prevention.

I. FACIAL RECOGNITION AS A NEW FORM OF BIOMETRICS

Compared to conventional identification methods such as ID, tokens, and passwords, biometric methods provide a much higher level of security and accuracy in terms of identification due to the uniqueness of biometric data[13]. In such, even though several international legal documents defined biometric data with different wordings so far, all of them basically focused on its uniqueness and special data processing technicality. While Convention for the protection of individuals with regard to the processing of personal data (Convention 108+) art. 6/1 does not provide a clear definition or align with the concept of "uniquely identifying a person", both the European Union's documents General Data Protection Regulation numbered 2016/679 (GDPR) art. 4/14 and Law Enforcement Directive numbered 2016/680 (LED) art. 3/13 precisely define:

> "personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural

12 *S and Marper v. The United Kingdom*, Applications nos. 30562/04 and 30566/04, 4 December 2008, para. 125.

13 Jain et al (n 1) 9.

> person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

Measurements of physiological and/or behavioural characteristics qualify as biometrics as long as they meet the requirements of universality, distinctiveness, permanence, and collectability[14].

Despite that genetic analysis on DNA, the shape of the ear and cartilaginous tissue of the pinna, hand geometry, scanning iris and retina, and storage of fingerprints on AFIS, and the captured images transfer via surveillance cameras to a facial recognition database[15] meet these criteria to be accepted as biometrics, the accuracy rates may vary on the applied biometric methods and condition of the data subject, whereas booking the fingerprints for a data subject who has no fingers or providing hand geometry for a signature from an illiterate person would apparently be infeasible[16].

As being one of the methods on biometrics FRT is widely recognized as a tool that utilizes

> "a technology that can detect and extract a human face from a digital image and then match this face against a database of pre-identified faces".

There are currently three distinct forms of this concept. To classify, first of all, one-to-one matching functions to match a human face extracted from a digital image against one pre-identified face, such as the smartphone's users are already familiar with unlocking the Face ID feature. Given that it is designed to only match a pre-identified face, one-to-one facial recognition does not pose a significant risk to the processing of additional personal data or the identification of potential unauthorized users[17]. Secondly, the one-to-many form of FRT excels in identifying a face from a crowd and matching it to an identity by comparing the captured face with a database containing thousands or even millions of faces.

---

14 Jain et al (n 1) 4; O. Iloanusi, and C. Osuagwu, 'Biometric Recognition: Overview and Applications' (2008) 27 (2) Nigerian Journal of Technology 37.

15 Jain et al (n 1) 8-10.

16 About these methods see Oliver Chevella N. and Kumar, Sajeesh, 'Biometric Technology Towards Prevention of Medical Identity Theft: Physicians' Perceptions' (2016) 5 (1) Health Informatics- An International Journal 13-14; Iloanusi and Osuagwu (n 13) 38.

17 Neil Selwyn, Mark Andrejevic, Chris O'Neill, Xin Gu, and Gavin Smith, 'Facial Recognition Technology Key Issues and Emerging Concerns' in Rita Matulionyte and Monika Zalnieriute (eds) *The Cambridge Handbook of Facial Recognition In The Modern State* (Cambridge University Press, 2024) 11; Giulia Gabrielli, 'The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights' (2025) (16) European Journal of Risk Regulation 517.

Indeed, mass surveillance commonly employs the one-to-many form of FRT[18]. The third form of FRT, known as facial processing, is more adept at assessing an individual's characteristics such as gender, race, age, emotional state, personality type, and behavioural intentions. Indeed, societies that experienced the COVID-19 pandemic and recognized high body temperature and virality symptoms reflected on the face found facial scanning to be nothing extraordinary[19].

II. THE LEGITIMATE REASONING BEHIND APPLICATION OF BIOMETRICS IN LAW ENFORCEMENT

The premise behind the use of biometrics is the concept of deterrence, as the Strasbourg Court, in its *Van Der Velden v. The Netherlands* decision, succinctly summarized the purpose of the Dutch DNA Testing (Convicted Persons) Act, which facilitates the processing of DNA profiles for the prevention, detection, prosecution, and trial of criminal offences. The Court stated that the purpose of retaining DNA profiles is

> "to assist in the solving of crimes, including bringing their perpetrators to justice, since, with the help of the database, the police may be able to identify perpetrators of offences faster, and to contribute towards a lower rate of reoffending, since a person knowing that his or her DNA profile is included in a national database may dissuade him or her from committing further offences"[20].

This reasoning continues to be applied in subsequent cases. In one of the landmark cases involving the use of biometrics for law enforcement, the Grand Chamber emphasized in *S. and Marper v. The United Kingdom* that while the collection of DNA information aids in the detection of a suspected individual and the commission of a crime, its detention serves a broader purpose. In its own words, "its retention pursues the broader purpose of assisting in the identification of future offenders"[21].

In fact, this reasoning aligns with Bentham's panopticon, albeit with slight modifications; rather than focusing on prisoners, it instills in everyone in society the awareness of surveillance as a means of committing an offence. This axiomatic idea is realized by CCTV cameras in every corner of the streets and the crowds from airports, stations, squares, and malls, whereas there is no thorough criminological research[22] or official statistics to indicate the relationship

---

18 Selwyn et al (n 16) 11-12.

19 Selwyn et al (n 16) 12.

20 *Van Der Velden v. The Netherlands*, paras. 6-7.

21 *S and Marper v. The United Kingdom*, para. 100.

22 *Shah et al* highlighted that algorithms like linear regression, additive regression, and decision

between public surveillance and crime rates. In an effort to mitigate the risk of oversurveillance, academic endeavours have proposed several solution. While some academics focused on criminogene, suggesting that instead of randomly selecting CCTV and FRT points, provinces should be selected based on factors such as public safety, hot spots with high crime rates, and the use of crime maps[23], others emphasized the importance of collaboration and consultation between neighbours and law enforcement authorities. Accordingly, unless structural measures such as lightening the area and hiring security staff are sufficient to prevent crimes, public surveillance should come to the fore.

To minimise the risk of oversurveillance, the application of these technologies could be allocated only for law enforcement agencies. Although not directly related to FRT, tracking phones via a stingray is one of the innovations applied for police surveillance purposes and is disputable in terms of the Fourth Amendment in the USA[24]. As the regulatory agency, the Federal Communications Commission intervened; the manufacturer of this technology turned out to follow these criteria: that the marketing and sale of the technology is only for the purpose of public safety to the local, state and federal extent and by law enforcement officials. Moreover, law enforcement agencies are subject to the authorisation of the FBI for acquisition and use of the device[25].

III. APPLYING A COST-BENEFIT APPROACH AND SEEK A FAIR BALANCE BETWEEN UTOPIA AND DYSTOPIA

A. Function Creep

The concerns from bias to discrimination are regarding the path towards a dystopia that stems from the phenomenon of "function creep"[26], which essentially implies that the function of FRT may be expanding beyond its original purpose of ensuring public safety. Qouting Smith and Mann

> "The roots of discrimination in policing do not stem entirely from the use of new technology in and of itself, but rather the institutions

stumps can be used to predict crime, and it's believed that machine learning techniques are good and precise for forecasting violent crime trends. See Shah et al (n 7) 3.

23 Nancy G. La Vigne, Samantha Lowry, Allison M. Dwyer, and Joshua A. Markman, *Using Public Surveillance Systems for Crime Control and Prevention* (Washington DC, The Urban Institute, 2011) 5.

24 Shah et al (n 7) 2.

25 Shah et al (n 7) 2-3.

26 For detailed information on this phenomenon, see Erbas (n 5) 339-340; for a semantic approach in detail, see Bert Jaap Koops, 'The Concept of Function Creep' (2021) 13 (1) Law, Innovation and Technology 30.

> of policing and the actions of police officers in discretionary and discriminatory enforcement of the law"[27].

implies the phenomenon as well as the narrative reflected in *Glukhin v. Russia* also implicitly hints at. In other words, bias or discrimination concerns does not inherently stem from the use of FRT; FRT is a tool that enables the repressive governments to use for their own goals to detect the ones being considered as a "threat" to them. However, the ECtHR's approach in *Glukhin v. Russia* is criticised for focussing too much on safeguards instead of FRT itself[28]. In reality, the safeguards come from concerns, which should also be carefully considered because of the imbalance of power between people who can use FRT and law enforcement agencies who can use it, as well as the possibility of misusing FRT[29]. Furthermore, procedural safeguards are not novel considering the ECtHR's juridprudence on biometric and genetic data protection, as the Court emphasized in *Gaughran v. The United Kingdom* that even though time limits for retention of such data fall within the margin of appreaciation of the state, it rested on certain safeguards for retention of data such as seriousness of offence, continuing need for retention, right to be deleted for personal data, data subject's age[30].

The Council of Europe's approach to mass surveillance is not rigid, as it does not inherently violate human rights, provided that its implementation aligns with the right to freedom of expression as well as the right to private life[31]. However, in the *Glukhin v. Russia* case, function creep primarily targeted political opponents, demonstrating a different approach from the conventional police approach. Rather than intervening with protestors and opponents, the police preferred gatherings to occur, capturing faces through face recognition technology. After a few days, the police initiated detentions, ultimately finding

---

27 Smith and Mann (n 3) 92.

28 *Zalnierute* refers to the ECtHR's stance as "procedural fetishism" and believes it oversimplifies the use of FRT. She attempts to highlight a hypothetical scenario in which both authoritarian and liberal states would legally accept the use of FRT, provided that procedural safeguards are already in place. In the end, this acceptance may impose a solid risk of misleading the public's attention rather than focusing on substantial questions about FRT. See. Monika Zalnieriute, 'Facial recognition technologies---freedom of expression--right to private life--surveillance--protest--biometric data--data privacy European Convention on Human Rights' (2023) 117 (4) American Journal of International Law 695-698.

29 Selwyn et al (n 16) 13.

30 *Gaughran v. The United Kingdom*, Application no. 45245/15, 13 February 2020, paras. 94-98.

31 Saadet Yuksel, 'New Technologies through a Human Rights Lens: Reflecting on Personal Autonomy and Non-Discrimination' (2022) 10 (2) Journal of Penal Law and Criminology 290.

the individuals involved guilty for their participation in the gatherings[32]. Other concerns can be expanded to include instances of discrimination reflected in the media, such as the use of FRT by police and security agencies, which has led to instances of racialized discrimination in the USA, fishing, and blacklisting of ethnic and religious minorities, such as the Uyghur population in China, or as a means of silencing political opponents in Myanmar[33]. For instance, people express concerns about discrimination against the Uyghurs, citing their unique appearance compared to the Han-descendant majority in China and the ease with which discrimination can occur after recording them. In other words, the concern emerges on the basis that FRT will automatically confront and follow the Uyghurs at every step[34] considering that China's giant database called Integrated Joint Operations Platform (IJOP) where individuals' personal data collected from a wide array of data sources including CCTV cameras, wifi sniffers, FRT, banking and health data in Xinjiang residents in the meantime collect mandatory DNA samples aged 12-65 there[35].

Feldstein's observation on FRTs' use by the governments actually summarizes with one word "unsurprisingly" and keeps on

> "countries with authoritarian systems and low levels of political rights are investing heavily in AI surveillance techniques. Many governments in the Gulf, East Asia, and South/Central Asia are procuring advanced analytic systems, facial recognition cameras, and sophisticated monitoring capabilities"[36].

Considering the mind-boggling amount of data processed by FRTs, function creep leads to concerns about privacy owing to the unique characteristics of biometric data, which may consist of information related to the health and ethnic

---

32 This narrative is based on the reflected case by Human Rights in Russia after a student participated in a rally in support of Russian opponent Navalnyy. See 'How the Russian state uses cameras against protesters' 17 January 2022 <https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters#1> accessed 20 January 2025. For detailed explanation about freedom of expression and right to assembly in accordance with international human rights law see. Gabrielli (n 17) 522 ff.

33 Selwyn et al (n 16) 13-14. For ethical challenges and bias on FRT see Pedro Robles, Daniel J. Mallinson, Eric Best, Cheryl Devaney, and Lauren Azevedo, 'Global Perspectives on Regulating Facial Recognition Technology Utilization for Criminal Justice Arrests' 5 (2025) Global Public Policy and Governance 189.

34 Paul Mozur, 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority' (New York Times, 2019) <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> accessed 17 January 2025.

35 Feldstein (n 4) 21.

36 Feldstein (n 4) 8.

origin of data subjects[37]. Using deep learning and facial analysis, it has up to a 96.6% correct matching rate in determining whether a person takes their pills or not or has a genetic disease such as DiGeorge syndrome[38].

B. Mismatches

The risk of discrimination may not only stem from function creep but also from the accuracy rates of the FRT itself, despite that FRT's correct matching rate increasing day by day in fascinating figures, such as in DeepFace, which was presented by Facebook in 2014 and had a 97.25 percent correct matching rate; the year after, FaceNet, which was presented by Google, had a 99.63 percent correct matching rate. In the meantime, using Google Photos, Facebook automatically tags people based on their recognition[39], and this increases the data and the possibility of correct matching rates even more. However the high mismatch rates are valid too as it reflected by an independent report of the United Kingdom's Metropolitan Police that FRTs error rates are nearly 81 percent, or Axon, USA police body camera supplier whose independent ethics board stated that "Face recognition technology is not currently reliable enough to ethically justify its use"[40]. In that, factors such as ageing, plastic surgery, cosmetics, image quality, a person's posture, and the camera's perspective can influence FRT's matching potential[41]. The age of the data subject affects the matching potential, as bone elasticity and shifts of children and adolescents who continue to grow up change more sharply. The National Institute of Standards and Technology's research on facial recognition algorithms also reveals a higher error rate when matching images of children.

Additionally, physical and environmental factors like sweaty or wet fingers, cuts on the fingers, or incomplete placement of the fingers on the censor briefly called noisy data can cause mismatches in biometric data[42]. A study on the Face2Rec smart glasses revealed that a data subject's angle too far from the camera could reduce image quality, and wearing glasses could potentially confuse the algorithm, thereby increasing the risk of mismatches[43].

---

37 Matthias Pocs, 'Legally compatible design of future biometric systems for crime prevention' (2013) 26 (1-2) Innovation: The European Journal of Social Science Research 44.

38 Thales Group, 'Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases and Latest News)' (2018) <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition> accessed 20 January 2025.

39 Thales Group (n 37).

40 Feldstein (n 4) 19.

41 Interpol, 'Facial Recognition' (2020) <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition.> accessed 20 January 2025 1; Smith and Mann (n 3) 89.

42 Jain et al (n 1) 6-14.

43 Gabriella A. Mayorga, Xuan Do, and Vahid Heydari, 'Using Smart Glasses for Facial Recognition' 15 (4) (2019) American Journal of Undergraduate Research 32.

In addition to physical and situational factors, the development of FRTs and the data they rely on raises concerns about potential racial discrimination against people of color. For example, the number of Black and Latino adolescents involved in juvenile criminal proceedings increased significantly in 2017. In fact, the Black adolescent rate is 15 times higher[44]. In 2017, Apple's Face ID faced criticism in China for its inability to distinguish Chinese faces[45]. Simultaneously, the police's use of facial recognition systems in Cardiff during the Champions League Final led to the incorrect detection of approximately 2000 people as suspects[46]. Additionally, the 2019 report from the National Institute of Standards and Technology revealed that the FRT's accuracy rates for African American and Asian faces are significantly low, resulting in a misidentification rate that ranges from 10 to 100 times higher[47]. FRTs' mismatching potential is affected by intersectionality as well, where the scanned picture belongs to women from minority groups as it emphasized that "the darker the skin, the more errors arise—up to nearly 35 percent for images of darker skinned women"[48].

This, of course, not only distorts the credibility of the FRT, but also poses a risk to the right to presumption and the right to liberty. The risk of how criminology's efforts by Lombroso in 19th-century people are based on metricising and pointing out visual markers of criminals[49]. FRTs contain such threat in the 21st century on the people the FRTs algorithm does not develop enough on accuracy. As one of the cases reflected by media shows, a theft suspect's image was recorded via CCTV camera. However, there was no match in the facial recognition database. The competent officer for the facial recognition system likened the suspect to a celebrity and uploaded the high-resolution picture of the celebrity from Google Images to the database. In this manner, the system established a match, leading to the arrest of the suspect[50]. This implies that, even in the absence of a match in the facial recognition database, the system may utilize a similar picture, someone else's picture, or a picture from Facebook. Should there be a potential mismatch, the individual may face arrest merely for resembling someone else. In fact, when a match is provided correctly, this does not result in disregarding

44 Joseph Goldstein and Ali Watkins, 'She Was Arrested at 14 Then Her Photo Went to a Facial Recognition Database' (2019) <https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.> accessed 15 January 2025.

45 Thales Group (n 37).

46 Ross Kelly, 'Facial Recognition Technology: Dystopia or Hysteria?' (2019) <https://digit.fyi/facial-recognition-technology-dystopia-or-hysteria/> accessed 17 January 2025.

47 Smith and Mann (n 3) 91.

48 Feldstein (n 4) 19.

49 Mareile Kaufmann and Maja Vestad, 'Biology and Criminology: Data Practices and the Creation of Anatomic and Genomic Body 'Types' (2023) 31 (4) Critical Criminology 1219.

50 Clare Garvie, 'Garbage In Garbage Out: Face Recognition on Flawed Data' (2019) <https://www.flawedfacedata.com/> accessed 18 January 2025.

the presumption of innocence. While what the match actually means is that one belongs to a certain face in the database, and other evidence should be corroborated with as well to solve the crime and convict the defendant[51].

Human rights activists have made several attempts to prohibit the use of FRT due to the aforementioned concerns. For instance, in London, they have argued that installing surveillance cameras and facial recognition systems in public spaces is both intrusive and dangerous for pedestrians. So much so that a passerby who covered his face in front of the camera has faced up with police intervention and been fined £90[52]. In the same vein, Amnesty International AI and human rights researcher emphasised,

> "Facial recognition risks being weaponised by law enforcement against marginalised communities around the world. From New Delhi to New York, this invasive technology turns our identities against us and undermines human rights"[53].

These efforts have also been successful in some parts of the world, such as San Francisco, where the prohibition of FRT stems from concerns that it interferes with civil rights, exacerbates racial discrimination, and jeopardizes the freedom to live without government monitoring[54].

However, FRT proponents have their own optimistic arguments. Without any doubt, the use of FRT has created a massive market and commercial interest; the proponents apply a wide array of compelling benefits of the FRT to society. The reasoning on FRTs use for crime prevention is also nourishing by each state's dynamics on threats with the support of tech companies. For instance, Huawei advertising its smart city public safety technologies puts its lenses to regional security issues as *Feldstein* emphasized that

> "in the Middle East, its platforms can prevent "extremism"; in Latin America, safe cities enable governments to reduce crime; and that in North America, its technology will help the United States advance "counterextremism" programs"[55].

---

51 Pocs (n 36) 40.

52 BBC News, 'Could Facial Recognition Cut Crime?' (2019) <https://www.bbc.co.uk/news/av/technology-48228677> accessed 12 January 2025.

53 The Guardian, 'Human rights group urges New York to ban police use of facial recognition' (2021) <https://www.theguardian.com/technology/2021/jan/25/new-york-facial-recognition-technology-police.> accessed 12 January 2025.

54 Amended In Committee 5/6/19 File No. 190110 Ordinance No. article 1/d. For detailed explanation about the situation in USA comparatively Canada, Germany, Italy, and France see Robles et al (n 33) 192 ff.

55 Feldstein (n 4) 17.

The pleaded benefits of FRT are mostly nourished by pro-social uses apart from prevention of crime or crime solving. One of the primary arguments in favor of FRT is its ability to locate individuals who are vulnerable, particularly those suffering from Alzheimer's, dementia, and similar diseases. The Thales Group, a reputable player in the electronics sector, praises this use. The reference picture provided by the missing person's family allows for a comparison with images in facial recognition databases, facilitating easy identification of the missing person[56]. *Atkinson*, aligned with Thales Group, portrays the FRT as more utopian than dystopian, depicting a Hollywood-style scenario where police officers check the child's family-provided picture in a national database for a positive match. The facial recognition system detects the child sitting near the kidnapper as he passes the tollbooth, triggering an automated signal to the police. Thirty miles ahead, police officers stop the car, capture the kidnapper, and deliver the child safely to their family[57].

Indeed, the San Diego County Sheriff's Department has implemented this argument, known as The Take Me Home Programme, for the benefit of the public, particularly those with autism, dementia, and various other personal situations. As a lost person is not able to speak or is unconscious, the police officer tries to detect whether they have any allergies, have a pacemaker or not, and reach family or relatives of the person by comparing their image with the images in the database and matching[58].

The pro-social uses could be even exemplified as "*They could also be used for navigation by giving them information about the distance"* considering wearable smart technologies[59]. The use of FRT in healthcare facilities provides societal benefits by maintaining socio-economic safety too. As social insurance systems are intrigued by the deterrent effect of biometrics, medical identity theft turns out to be devastating costs on the system prevalent in societies where healthcare services charge a high amount of money and the social insurance system is not inclusive for the underprivileged[60]. Rather than health insurance cards or social security numbers, biometric technologies seemed to be a resolvent for this crime

56 Thales Group (n 37).

57 Robert D. Atkinson, 'Facial-Recognition Technology: Closer to Utopia Than Dystopia' (2019) <https://www.nationalreview.com/2019/11/facial-recognition-technology-closer-to-utopia-than-dystopia/> accessed 12 January 2025.

58 Anthony M. Carter, 'Facing Reality: The Benefits and Challenges of Facial Recognition' Master Thesis, (California, 2018) <https://apps.dtic.mil/sti/trecms/pdf/AD1065272.pdf> accessed 10 February 2025.

59 Hermann Schweizer, 'Smart glasses: technology and applications' (2014) <https://vs.inf.ethz.ch/edu/FS2014/UCS/reports/HermannSchweizer_SmartGlassesTechnologyApplications_report.pdf> accessed 16 February 2025 4.

60 Oliver and Kumar (n 15) 11.

phenomenon[61]. Another pro-social benefit is the reduction of bureaucracy and paperwork, such as the common use of one-to-one FRT for electronic passport and visa checks at airports without waiting in long lines, or the use of face IDs for book borrowing from libraries and paying for canteens at campuses[62].

Given the extensive use of FRTs for pro-social purposes, crime prevention, and criminal capture, it's plausible that the rapid advancements in these technologies could overshadow concerns about mismatching rates. Indeed, technical developments on FRTs may easily handle the issues stemming from mismatching and its ramifications for minorities. Even at present, despite the limitations of existing technologies, states' enthusiasm for FRTs seems to indicate that concerns about function creep and mismatches do not deter them from implementing them. However, the concern about states misuse or abuse is not anything novel and could have been dated back to struggles in human rights history, even if the function creep mostly corresponds to developing technology cases. That's why the inevitable everyday use of FRTs paves the way for a dystopian approach to mass surveillance. To that extent, the authoritarian state's reluctance[63] toward freedoms would turn into an oxymoronic way, where people wanting to stand up for civil liberties against mass surveillance may not even enjoy freedom of assembly to form public opinion because of the chilling effect of FRTs.

---

61 Oliver and Kumar (n 15) 14.

62 Selwyn et al (n 16) 16.

63 States' reluctance extends beyond the freedom of assembly to other spheres of human rights, as exemplified by a case from Turkiye, which highlights their positions against human rights. Code of Social Insurance and General Health Insurance numbered 5510 enables biometric identity verification. Article 67/3 of the Code stipulates that when the insured and those under their care apply to healthcare providers, they must undergo identity verification using biometric methods or documents, such as an identity card or driving license, unless an emergency occurs. Even in emergency situations, the verification process should continue after the emergency situation has passed. Yet, while the mentioned article was promulgated, there was no personal data protection code in Turkiye, and this resulted in a constitutional objection to the article before the Turkish Constitutional Court in terms of the interference being in accordance with the law. The Court ruled that the article did not violate the right to respect private and family life, citing the safety of biometric methods against unauthorized use and their ability to prevent corruption in public authorities given the inadequacy of existing methods for identity verification. However, the Court disregarded the fact that the data protection code was not available until 2016, which resulted in a lack of protection for personal data subjects. This was due to the absence of a clear provision for the data processing regime, the data subjects' rights, the controller's obligations, and the conditions of data transfer. Consequently, the processing of individuals' biometric data was not in accordance with the law, as a single article 67/3 was insufficient to protect the data subject and did not meet these quality of law requirements. See the judgment of Turkish Constitutional Court, E. 2014/180, K. 2015/30, 19.3.2015.

As Mayorga et al emphasized that;

> "As long as the technology is used to protect citizens and not abused, facial recognition can be extremely beneficial"[64].

The lesson derived from the history of human rights could fulfill this "as long as". As the protection of human rights is inherently enshrined in several human rights documents, including the European Human Rights Convention, which already covers biometric data protection, the 108+ Convention, the GDPR, and the LED. These documents conceptualize data processing principles such as processing lawfully and fairly, collecting for specified, explicit, and legitimate purposes, minimising data, keeping data up to date, adhering to the time limits principle, and implementing other appropriate safeguards unique to the special categories of personal data, including biometric and genetic data. Following safeguards in data processing can tame the state's tendency towards function creep.

CONCLUSION

Public surveillance and facial recognition systems, which have become a part of our lives, process biometric data of individuals at any time. These technologies enable rapid identification and arrest of criminals, thereby enhancing the efficiency of law enforcement and criminal justice mechanisms worldwide. Furthermore, these systems aim to deter individuals from committing crimes by making them aware of the ease of police capture, thereby providing long-term deterrence. However, evaluating the effectiveness of these systems in terms of deterrence is difficult due to the lack of criminological studies specifically focused on crime prevention. In such a way that it risks that the governments disguise their repressive purposes behind this apparent purpose of preventing crime, and the world turns into a panopticon, or even worse for both guilty and innocent people.

To mitigate the risks and concerns of privacy, discrimination, and function creep, several states and human rights activists have tackled the issue by prohibiting FRT. However, a complete ban is unfeasible, as it would deprive the prohibited areas of the opportunity to apprehend criminals. Rather than completely prohibiting the use of these systems, the ECtHR's stance on procedural safeguards and its outline of the principles of processing personal data could be an option for states to apply, including data minimization, processing for specific, explicit, and legitimate purposes, setting time limits, and providing guarantees to data subjects. Given that the age and race of an individual significantly influence the correct match rate of the FRTs algorithm, and that the images of children and adolescents may undergo significant changes as they mature, it is advisable to

[64] Mayorga et al (n 42) 24.

retain the data processed for these groups of people for a shorter period of time, in accordance with the principles of time limit and proportionality.

BIBLIOGRAPHY

Atkinson RD, 'Facial-Recognition Technology: Closer to Utopia Than Dystopia' (2019) <https://www.nationalreview.com/2019/11/facial-recognition-technology-closer-to-utopia-than-dystopia/> accessed 12 January 2025

BBC News, 'Could Facial Recognition Cut Crime?' (2019) <https://www.bbc.co.uk/news/av/technology-48228677> accessed 12 January 2025

Carter, AM, 'Facing Reality: The Benefits and Challenges of Facial Recognition' Master Thesis, (California, 2018) <https://apps.dtic.mil/sti/trecms/pdf/AD1065272.pdf> accessed 10 February 2025

Erbas R, 'DNA Databases For Criminal Justice System: A Pathway Towards Utopian or Dystopian Future?' (2022) (18) The Age of Human Rights Journal, 331-343

Feldstein S, 'The Global Expansion of AI Surveillance' (2019) Carnegie Endowment For International Peace <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en> accessed 21 December 2024

Gabrielli G, 'The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights' (2025) (16) European Journal of Risk Regulation 514-541

Garvie C, 'Garbage In Garbage Out: Face Recognition on Flawed Data' (2019) <https://www.flawedfacedata.com/> accessed 18 January 2025

Goldstein J and Watkins A, 'She Was Arrested at 14 Then Her Photo Went to a Facial Recognition Database' (2019) <https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.> accessed 15 January 2025

Iloanusi O, and Osuagwu C, 'Biometric Recognition: Overview and Applications' (2008) 27 (2) Nigerian Journal of Technology, 36-45

Interpol, 'Facial Recognition' (2020) <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition.> accessed 20 January 2025

Jain AK, Ross A, and Prabhakar S, 'An Introduction to Biometric Recognition' (2004) 14 (1) IEEE Transactions on Circuits and Systems for Video Technology 4-20

Kaufmann M and Vestad M, 'Biology and Criminology: Data Practices and the Creation of Anatomic and Genomic Body 'Types' (2023) 31 (4) Critical Criminology 1217-1232

Kelly R, 'Facial Recognition Technology: Dystopia or Hysteria?' (2019) <https://digit.fyi/facial-recognition-technology-dystopia-or-hysteria/> accessed 17 January 2025

Koops BJ, 'The Concept of Function Creep' (2021) 13 (1) Law, Innovation and Technology 29-56

La Vigne NG, Lowry S, Dwyer AM, and Markman JA, *Using Public Surveillance Systems for Crime Control and Prevention* (Washington DC, The Urban Institute, 2011)

Li P and Cadell C, 'China Eyes 'Black Tech' To Boost Security As Parliament Meets' (Reuters, 2018) <https://www.reuters.com/article/technology/china-eyes-black-tech-to-boost-security-as-parliament-meets-idUSKBN1GM06M/> accessed 15 December 2024

Marciano A, 'Reframing biometric surveillance: from a means of inspection to a form of control' (2019) (21) Ethics and Information Technology 127-136

Mayorga GA, Do X and Heydari V, 'Using Smart Glasses for Facial Recognition' 15 (4) (2019) American Journal of Undergraduate Research 23-35

Mozur P, 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority' (New York Times, 2019) <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> accessed 17 January 2025

Oliver CN and Kumar S, 'Biometric Technology Towards Prevention of Medical Identity Theft: Physicians' Perceptions' (2016) 5 (1) Health Informatics- An International Journal 11-22

Orwell G, *1984* (Arcturus Publishing, 2013)

Pocs M, 'Legally compatible design of future biometric systems for crime prevention' (2013) 26 (1-2) Innovation: The European Journal of Social Science Research 36-56

Robles P, Mallinson DJ, Best E, Devaney C, and Azevedo L, 'Global Perspectives on Regulating Facial Recognition Technology Utilization for Criminal Justice Arrests' 5 (2025) Global Public Policy and Governance 186-204

Schweizer H, 'Smart glasses: technology and applications' (2014) <https://vs.inf.ethz.ch/edu/FS2014/UCS/reports/HermannSchweizer_SmartGlassesTechnologyApplications_report.pdf> accessed 16 February 2025

Selwyn N, Andrejevic M, O'Neill C, Gu X, and Smith G, 'Facial Recognition Technology Key Issues and Emerging Concerns' in Rita Matulionyte and Monika Zalnieriute (eds) *The Cambridge Handbook of Facial Recognition In The Modern State* (Cambridge University Press, 2024) 11-29

Shah N, Bhagat N and Shah M, 'Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention' (2021) 4 (9) Visual Computing for Industry, Biomedicine, and Art 1-14

Smith M and Mann M, 'Facial Recognition Technology and Potential for Bias and Discrimination' in Rita Matulionyte and Monika Zalnieriute (eds) *The Cambridge Handbook of Facial Recognition In The Modern State*, (Cambridge University Press, 2024)

Springwise, 'Chinese Police Adopt Smart Glass Technology' (2018) <https://www.springwise.com/chinese-police-adopt-smart-glass-technology/#:~:text=Using%20facial%20recognition%20technology%2C%20these,technology%20to%20assist%20police%20work> accessed 15 December 2024

Thales Group, 'Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases and Latest News)' (2018) <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition> accessed 20 January 2025

The Guardian, 'Human rights group urges New York to ban police use of facial recognition' (2021) <https://www.theguardian.com/technology/2021/jan/25/new-york-facial-recognition-technology-police.> accessed 12 January 2025

Yuksel S, 'New Technologies through a Human Rights Lens: Reflecting on Personal Autonomy and Non-Discrimination' (2022) 10 (2) Journal of Penal Law and Criminology 281-305

Zalnieriute M, 'Facial recognition technologies---freedom of expression--right to private life--surveillance--protest--biometric data--data privacy European Convention on Human Rights' (2023) 117 (4) American Journal of International Law 695-701